Chapter 16
A Framework for Image Encryption on Frequency Domain

Zhe Liu
Auckland University of Technology, New Zealand

Mee Loong Yang
Auckland University of Technology, New Zealand

Wei Qi Yan
Auckland University of Technology, New Zealand

ABSTRACT

In this chapter, the authors propose an improved image encryption algorithm based on digital watermarking. The algorithm combines discrete wavelet transform (DWT), discrete cosine transform (DCT), and singular value decomposition (SVD) together in a DWT-DCT-SVD framework to improve the robust watermarking technique. The secret image is embedded into both high-frequency and low-frequency sub-bands of the host image; this makes it difficult to be attacked in all the sub-bands. To reduce the size of a secret key, the authors use a logistic map to generate random images so as to replace the host images. They tested the algorithm by using five types of attacks and the results indicate that the proposed algorithm has higher robustness than traditional chaotic scrambling method and the DRPE method. It shows strong resilience against the five types of attacks as well as statistical attacks.

INTRODUCTION

Image encryption techniques can be divided into two groups. One group operates in spatial domain while the other in frequency domain. Earlier encryption methods work typically using chaotic logistic maps which require large amount of computations.

DOI: 10.4018/978-1-7998-7705-9.ch016

Generally, in these methods, discrete cosine transform (DCT) and discrete wavelet transform (DWT) are widely adopted because DCT avoids complex calculation compared with traditional discrete Fourier transform (DFT) (Ahmed, Natarajan, & Rao, 1974), and DWT can obtain good properties of input image in both spatial and frequency domain (Burrus, Gopinath, & Guo, 1998). They provide convenience for image encryption based on spatial and frequency domain.

We are aware that digital watermarking in frequency domain has high robustness. The basic workflow of digital watermarking is similar to image encryption and decryption processes. In this book chapter, we propose a new encryption method based on watermarking techniques, the encrypted and decrypted processes are designed by using a robust watermarking scheme which is called DWT-DCT-SVD framework. We also extend our method using chaotic map to generate the encryption/decryption images and reduce the size of the secret key. We carried out a series of experiments and found that the proposed method has higher robustness than DRPE method using DFT and DCT.

BACKGROUND

Since mainstream methods for image encryption and digital watermarking focus on frequency domain, we will outline these methods in this section. In 2017, three optical encryption schemes based on DRPE by using DWT were proposed (Mohamed, Samrah & Allah, 2017). These schemes were based on DRPE by using DWT and chaotic maps; one of them used DWT instead of fast Fourier Transform (FFT) in traditional DRPE. Another used DWT and steganography combined technique, and the last one utilized fractional fast Fourier transform (FRFFT), DWT and steganography together. The results were compared with three traditional techniques. From the performance metrics, the proposed three methods based on DWT achieved better performance and robustness versus conventional ones.

DCT has strong energy concentration characteristics in the low-frequency part. DCT is widely used in image processing such as image compression and image encryption. Compared with DFT, the computations of DCT are in real domain. Thus, DCT can resist geometric attack effectively. Because of these advantages, DCT has outstanding performance in the field of image encryption. In 2010, an image encryption algorithm was proposed based on Arnold transform and DCT (Liu, et al., 2011). In 2011, an image encryption algorithm using DCT and Secure Hash Algorithm-1 (SHA-1) was proposed (Yuen and Wong, 2011).

A watermarking algorithm for digital images based on DWT-DCT-SVD framework was proposed (Yuan and Zhou, 2011)(Wang, et al., 2009) where a four-layer DWT was applied to a secret image. Firstly, the low-frequency subband and three high-frequency subbands of the fourth layer were chosen. Similarly, the same operation was applied to the watermarking image. By using DCT and SVD, the four subbands obtained from the watermarking image were embedded into the host image adaptively. Finally, the watermarked image is obtained after the inverse SVD, DCT and DWT. Compared with the methods by using DCT-SVD and DWT-SVD frameworks, the experiments show that this method is more robust against geometric attacks.

Different from the existing methods for image encryption and image watermarking, we combine DCT, DWT and SVD together and form an image encryption scheme. Our method is robust to resist several kinds of attacks.